REMARKS

Claims 1-32 are all of the claims presently pending in the application. Claims 1, 10-12, 16, 20-21, 24, and 30-32 have been amended to more particularly define the invention.

It is noted that the claim amendments are made only for more particularly pointing out the invention, and not for distinguishing the invention over the prior art, narrowing the claims or for any statutory requirements of patentability. Further, Applicant specifically states that no amendment to any claim herein should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 1-32 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Chang, et al. (U.S. Patent No. 6,532,541) (hereinafter "Chang").

This rejection is respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

The claimed invention (e.g., as exemplarily defined by claim 1) is directed to a method for generating an output file from a source file where benign modifications to a content of the output file still render the output file authentic. The method includes constructing an index vector from the source file, creating quantization functions based on the index vector and quantizing the source file using the quantization functions, generating an authentication mark from the quantized source file and the index vector, generating an authentication tag by appending the index vector to the authentication mark and generating the output file by appending the authentication tag to the source file.

Conventional robust authentication systems are used to verify the integrity of data by determining if the data survives incidental modifications such as lossy compression-decompression, noise, printing and scanning. Most conventional robust authentication schemes can be classified into two classes, based on the way they perform data reduction.

The first class performs data reduction by extracting some relevant features from the data and uses them in the authentication tag. In general, the source image does not need to be modified significantly in order for the image to be authenticatible. A drawback of this type of system is that because small changes in the image result in small changes in the tag, it is potentially easy to find forged images which generate the same or similar tags as the original image.

A second type of authentication system utilizes a cryptographic hash function to reduce the data and generate a relatively small tag from the image. This type of system modifies the source image significantly in order for the image to be authenticable. The amount of authenticability distortion applied to the image can be as large as the maximum amount of modification to the image that the authentication system is willing to tolerate before the image is deemed inauthentic.

The claimed invention of exemplary claim 1, on the other hand, provides a method for generating an output file from a source file including <u>creating quantization functions based on the index vector and quantizing the source file using the quantization functions</u> (e.g., see Application at page 5, lines 14-20). This allows the present invention to provide a robust authentication method that survives minor modifications to the data which combines the advantages of the two types of conventional classes of robust authentication systems (see Application at page 4, lines 8-11).

II. THE PRIOR ART REFERENCE

The Examiner alleges that Chang teaches the claimed invention of claims 1-32. Applicant submits, however, that there are elements of the claimed invention which are neither taught nor suggested by Chang.

That is, nowhere does Chang teach or suggest "*creating quantization functions based on the index vector and quantizing said source file using said quantization functions*" as recited in claim 1 and similarly recited in claims 20-21, 24, and 30-32.

As noted above, the claimed invention of exemplary claim 1, provides a method for generating an output file from a source file including <u>creating quantization functions based on the index vector and quantizing the source file using the quantization functions</u> (e.g., see Application at page 5, lines 14-20). This allows the present invention to provide a robust authentication method that survives minor modifications to the data which combines the advantages of the two types of conventional classes of robust authentication systems (see Application at page 4, lines 8-11).

The Examiner attempts to rely on several passages of Chang to support her allegations. Specifically, the Examiner alleges that Chang teaches quantizing a source file. The Examiner attempts to rely on column 5, lines 31-33 and 46-47 of Chang for providing support for this feature.

Nowhere, however, in this passage (nor anywhere else for that matter) does Chang teach or suggest a method for generating an output file from a source file including creating quantization functions based on the index vector and quantizing the source file using the quantization functions. Indeed, the Examiner does not even allege that Chang teaches or suggests this feature. In fact, the Examiner merely alleges that Chang teaches quantizing the source files.

Applicant's invention quantizes the data by using quantization functions that depend on features of a specific image. In particular, the claimed invention quantizes data according to the index vector, which in turn is computed from the source file (e.g., an image in an exemplary embodiment).

On the other hand, Chang teaches using a single quantization table throughout the entire image (see Chang at column 5, lines 31-33 and 46-47). Consequently, the method disclosed in Chang will only tolerate benign modification due to quantization, such as is done in JPEG compression. Other types of benign modifications such as brightening the image will not work with Chang's method. In contrast, because the invention includes creating quantization functions, the claimed invention allows the method to tolerate other types of benign modifications. Chang does not teach or suggest using an index vector to determine which quantization functions are used.

Regarding claim 2, the Examiner alleges that Chang teaches inserting the authentication tag to the source file by a robust data hiding algorithm. The Examiner attempts to rely on column 6, lines 62-65 to support her allegations. The Examiner, however, is incorrect.

That is, Chang does not teach or suggest inserting the authentication tag to the source file by a robust data hiding algorithm. Chang merely describes the generation of a signature, but does not discuss, teach or suggest inserting the signature back into the image. For example, in Figure 4 of Chang, the signature is a separate piece of information which needs to be supplied during authentication, whereas in the exemplary embodiment of the present invention defined by claim 2, the signature is embedded into the image or data.

Moreover, regarding claim 13, the Examiner alleges that Chang teaches that no distortion is added to the source file to generate the output file. The Examiner attempts to rely on column 5, lines 38-45 to support her allegations. The Examiner, however, is clearly incorrect.

That is, Chang does not teach or suggest that no distortion is added to the source file to generate the output file. Chang teaches JPEG compression, which invariably introduces distortion.

Furthermore, Chang does not teach or suggest a method for generating an output file from a source file including "*quantizing said feature vector according to the index vector*" as recited in exemplary independent claim 22.

The Examiner attempts to rely on Chang as suggesting quantizing the feature vector according to the index vector. The Examiner attempts to rely on column 5, lines 31-33 and 46-47 to support her allegations. The Examiner, however, is clearly incorrect.

That is, Chang does not teach or suggest quantizing the feature vector according to the index vector as in claim 22. Chang merely describes a common quantization table where all of the feature vectors are quantized the same way.

Therefore, Applicant submits that there are elements of the claimed invention that are not taught or suggest by Chang. Therefore, the Examiner is respectfully requested to withdraw this rejection.

III. FORMAL MATTERS AND CONCLUSION

In view of the foregoing, Applicant submits that claims 1-32, all of the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: October 1, 2004

Scott M. Tulino, Esq.
Registration No. 48,317

Sean M. McGinn, Esq.
Registration No. 34,386

McGinn & Gibb, PLLC
Intellectual Property Law
8321 Old Courthouse Road, Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254